Math 116: Problem Set 5

Owen Jones

2/20/2024

1. $\phi(11413) = \phi(101)\phi(113) = 100 \cdot 112 = 11200$ $\gcd(7467, 11200) = 1 \Rightarrow$

$$\begin{array}{ccc} & x & y \\ 11200 & 1 & 0 \\ 7467 & 0 & 1 \\ 3733 & 1 & -1 \\ 1 & -2 & 3 \end{array}$$

   $\Rightarrow \phi(11413) \mid 7467 \cdot 3 - 1$
   $\Rightarrow d = 3$ is our private key.
   Thus, 1415 is our plaintext.

2. $\phi(55) = 40 \Rightarrow 1 \cdot 40 + (-13) \cdot 3 = 1 \Rightarrow d = 27$

3. (a) Every letter is encrypted to a different number modulo n. Knowing the public key (e, n), we can create a dictionary of number letter pairs, and match each ciphertext number to its corresponding letter.

   (b)

$$\begin{array}{ccccc} A = 1 & B = 8192 & C = 4624 & D = 4028 & E = 794 \\ F = 2343 & G = 231 & H = 4461 & I = 4809 & J = 3556 \\ K = 476 & L = 2015 & M = 513 & N = 699 & O = 3603 \end{array}$$

   HELLO is our plaintext.

4. $a^1 \equiv a \pmod{n}$ for all a. Thus, $e = 1$ doesn't encrypt the plaintext. $\phi(n) = p_1^{e_1 - 1}\phi(p_1) \dots p_k^{e_k - 1}\phi(p_k)$. $\phi(p) = p - 1$ is an even number for any odd prime, so $\phi(n)$ is even. Thus, $e = 2$ is not relatively prime to $\phi(n)$.

5. Becuase e is suitably chosen, this means $\gcd(e, \phi(p)) = 1$. Use extended Euclidean algorithm to find integer d s.t $de \equiv 1 \pmod{\phi(p)}$. Because p is prime, $\phi(p) = p - 1$. The security of RSA relies on n being difficult to factor. i.e $\phi(n)$ is hard to compute. However, primes are very easy to factor because all their factors are trivial, 1 and p. Thus, p is a poor choice to be used in an RSA encryption.

6. $(2^e c)^d = 2^{ed}(m^e)^d = 2^{1+k\phi(n)} m^{1+k\phi(n)} \equiv 2m \pmod{n}$. Since n is a product of two odd primes, n is odd, so 2 and n are coprime. Thus, we can use the extended Euclidean algorithm to find 2's multiplicative inverse modulo n. $2' \cdot 2m \equiv m \pmod{n}$ which gives us Nelson's original message. We can consider this a chosen ciphertext attack.

7. (a) Eve can compute x^{-e} using the extended Euclidean algorithm because $x^{-e}x^e \equiv 1 \pmod{n}$. Let $m^c = 10^{100e} \pmod{n}$. She creates two lists $cx^{-e} \pmod{n}$ for $1 \leq x \leq 10^9$ and $m^c y^e \pmod{n}$ for $1 \leq y \leq 10^9$. If there is a match between the two lists, $m = xy$.

   (b) Let L be the length of the message m. $m \| m = m(10^L + 1)$. Let $m^c = \left(10^L + 1\right)^e \pmod{n}$. She creates two lists $cx^{-e} \pmod{n}$ for $1 \leq x \leq 10^9$ and $m^c y^e \pmod{n}$ for $1 \leq y \leq 10^9$. If there is a match between the two lists, $m = xy$.

8. If e_A and e_B are relatively prime, there exist integers x, y s.t $xe_A + ye_B = 1$. It follows $c_A^x \cdot c_B^y \equiv m^{xe_A} m^{ye_B} \equiv m^{xe_A + ye_B} \equiv m \pmod{n}$.

9. (a) If M is a multiple of $p-1$ and $q-1$, there exists integers k_1 and k_2 s.t $M = k_1(p-1)$ and $M = k_2(q-1)$. By Fermat's little theorem, $a^M \equiv \left(a^{p-1}\right)^{k_1} \equiv 1 \pmod{p}$, and the same idea holds for q. Because $a^M \equiv 1 \pmod{p}$ and $a^M \equiv 1 \pmod{q}$, the Chinese remainder theorem guarantees a unique solution $a^M \equiv x \pmod{n}$ for some x. Because $a^M = 1 + kpq$ for some k satisfies the system of system of congruences, $x = 1$ must be the unique solution modulo n.

   (b) If $ed \equiv 1 \pmod{M}$ then $a^{ed} \equiv a^1 \cdot a^{kM} \equiv a^1 \cdot \left(a^M\right)^k \equiv a \pmod{n}$

10. $880525^2 \cdot 2057202^2 \equiv 6 \pmod{2288233}$
    $\Rightarrow 2288233 \mid (880525 \cdot 2057202 - 648581)(880525 \cdot 2057202 + 648581)$
    $\gcd(880525 \cdot 2057202 - 648581, 2288233) = 1871$ is a non-trivial factor of 2288233. The other factor is 1223.

11. Given $m^{12345} \equiv 1 \pmod{n}$, we know $ord(m) \mid 12345$. We want to find d st. $ed \equiv 1 \pmod{ord(m)}$. Since $\gcd(12345, e) = 1$, pick $d \equiv e^{-1} \pmod{12345}$ using the extended Euclidean algorithm. Thus, $c^d \equiv m^{ed} \equiv m^{12345k+1} \equiv \left(m^{12345}\right)^k \cdot m \equiv m \pmod{n}$.

12. (a)
$$m' \equiv m_1 \equiv c^{d_1} \equiv m^{ed_1} \equiv m^{1+k_1(p-1)} \equiv m \pmod{p}$$
$$m' \equiv m_2 \equiv c^{d_2} \equiv m^{ed_2} \equiv m^{1+k_2(q-1)} \equiv m \pmod{q}$$

    for integers k_1, k_2. By the uniquess of CRT, $m' = m + kpq$ for some integer k satisfies the system of congruences. Thus, $m' \equiv m \pmod{n}$

    (b) $m' = m_1 qy + m_2 px \pmod{n}$.

13. 6010320151809140709190801180

14. $n = 835338435834994481423891073871 \times 897930023819537415148640533529$

15. $2, 3$, and 5 all fail to show n is composite $7^{n-1} \equiv 10334100 \pmod{n}$

16. (a) For bases $b = 2, 3$ $b^{n-1} \equiv 1 \pmod{n}$, so we conclude n is probably prime.

(b) Base $b = 3$ proves n is composite giving non-trivial factor 520801. Other factor is 3361.

In [1]:

```
import numpy as np
import math116
```

In [2]:

```
n_13=67978778462897780371924622182706779 7
```

In [5]:

```
d_13=math116.inverse(e_13,phi_n_13)
```

In [23]:
```
pow(7,n_15-1,n_15)
```
Out[23]: 10334100

In [24]:
```
n_16=1750412161
```

In [25]:
```
pow(2,n_16-1,n_16)
```
Out[25]: 1

In [26]:
```
pow(3,n_16-1,n_16)
```
Out[26]: 1

In [27]:
```
k_16=0
q_16=n_16-1
while q_16%2==0:
    q_16//=2
    k_16+=1
```

In [29]:
```
a_0_3=pow(3,q_16,n_16)
```

In [32]:
```
a_0_2=pow(2,q_16,n_16)
for i in range(k_16):
    if pow(a_0_2,2,n_16)==n_16-1:
        break
    elif pow(a_0_2,2,n_16)==1:
        print(math116.gcd(a_0_2-1,n_16))
        break
    a_0_2=pow(a_0_2,2,n_16)
```

In [33]:
```
a_0_3=pow(3,q_16,n_16)
for i in range(k_16):
    if pow(a_0_3,2,n_16)==n_16-1:
        break
    elif pow(a_0_3,2,n_16)==1:
        print(math116.gcd(a_0_3-1,n_16))
        break
    a_0_3=pow(a_0_3,2,n_16)
```
520801

In [34]:
```
n_16//520801
```
Out[34]: 3361

In [ ]: